

Encryption Options

03/19/2007

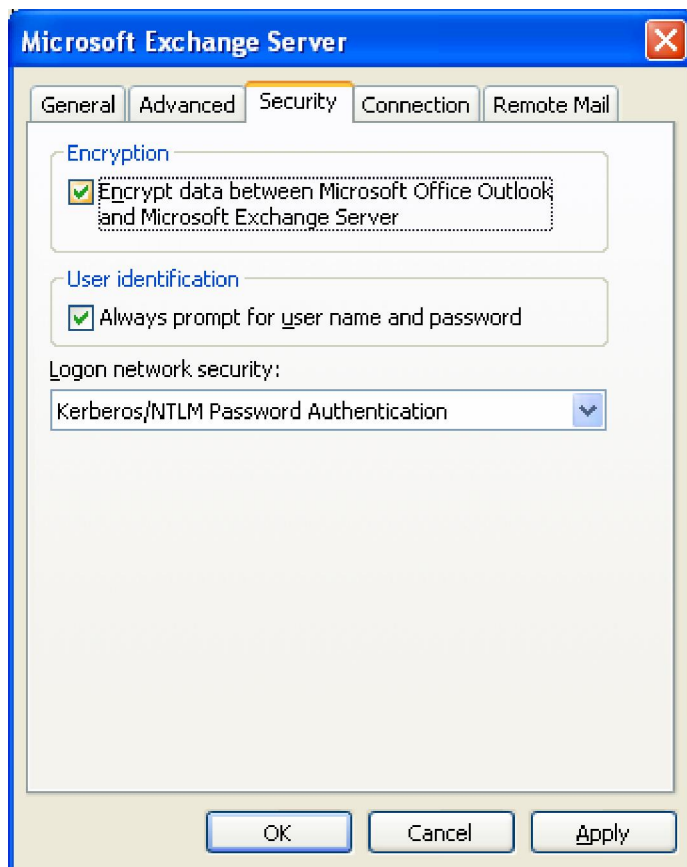
Table of Contents

Encrypt data between Outlook and Exchange.....	3
Secure Web Delivery (SWD).....	4
Requesting Security Certificates (Internal).....	8
Requesting Security Certificates (External).....	9
Administrator Portion.....	9
User Portion.....	14
Publishing Digital Signatures to the GAL.....	19
Digitally Signing Messages.....	20
Encrypting Messages with Outlook.....	21
Using S/MIME Controls with OWA.....	22

There are several different options for encrypting email. Which one is most appropriate for you depends on several factors. The biggest factor is whether you are sending email to another State of Alabama employee located on ACE or an external user. We have compiled most of these different options below. Some are easy to configure, and some are slightly more technical.

One of the easiest ways to add additional security to your messages is to configure Outlook to encrypt data sent between your client and the Exchange server. To do so:

1. In Outlook, open up Tools> Email Accounts> Next> Change> More Settings.
2. Click on the Security tab and place a check mark in the Encryption checkbox. Click OK to save changes.



This will encrypt your message until it gets to our Exchange server, but will not necessarily encrypt it when it is sent to an external user. Our outbound mail gateway will first try to send any message securely using SSL/TLS. However, if the receiving server does not have a suitable Security Certificate, or cannot accommodate a secure connection for any reason, it will send the message in clear text. We do have the capability of forcing mail to certain domains to be sent over a secure channel. In these cases, the message will not be sent if our server cannot establish a secure connection to the receiving mail server. If you would like to set this up, please contact our Help Desk at help.desk@isd.alabama.gov.

As mentioned above, this is all contingent upon the ability of the receiving mail server to support SSL/TLS. Another option we have is our Secure Web Delivery (SWD) server, which is designed to provide a secure alternative to server-to-server encryption.

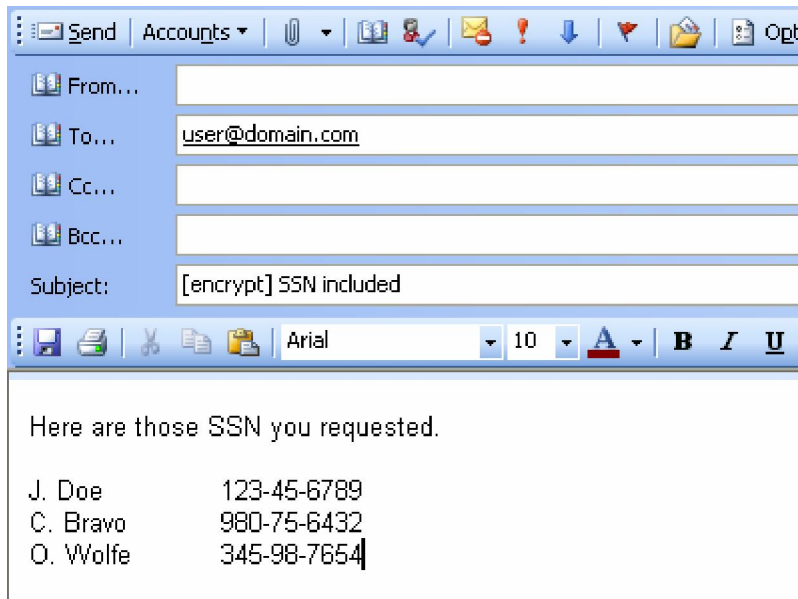
What is Secure Web Delivery (SWD)?

The SWD server allows you to securely email sensitive data to recipients outside of our email system. Outbound messages using SWD are intercepted before leaving our network. A notification is then sent to the intended recipient. This notification includes a link to your message, plus instructions.

Once the recipient clicks on the included link, they will be prompted for their username and password to ensure validity. After entering these credentials they can view your message through a web browser, reply to you, and manage any other messages they may have been sent securely. Recipients cannot forward your message on to any other users. They can only reply to you.

How Do I Send a Message Through the SWD?

The SWD is triggered based on subject-based filters. In other words, you have to request a message be sent through SWD by including *[encrypt]* in the subject line of your message. Then send the message as you normally would. **NOTE** The brackets are required.



Send Accounts [Attachment Icon] [Image Icon] [Link Icon] [Warning Icon] [Download Icon] [Folder Icon] Options

From: [Empty Field]

To: user@domain.com

Cc: [Empty Field]

Bcc: [Empty Field]

Subject: [encrypt] SSN included

[New] [Print] [Cut] [Copy] [Paste] Arial 10 [Font Color Icon] [Bold] [Italic] [Underline]

Here are those SSN you requested.

J. Doe	123-45-6789
C. Bravo	980-75-6432
O. Wolfe	345-98-7654

You will then receive a confirmation email that your message has been accepted by SWD.

Secure Web Delivery Notification

☒ Secure Web Delivery

To:

Your message sent on Thu Mar 15 10:26:36 2007 to user@domain.com has been marked as requiring encrypted delivery. Instructions for reviewing your message will be sent to the recipient. You will be notified if they have not accessed your message within two days.

The recipient will receive a message similar to the one below. If it is the first time they have received a message sent to them through SWD, the recipient will have to create a user account to ensure proper authentication for future deliveries. Otherwise, they will need to enter the credentials they have previously established. There is a link to click if the user has forgotten their password too.

Encryption Options

Click the link to view the secure web delivery

[View Message](#)

You will be prompted for your email address and password to protect your account.

Click on the link below if you have forgotten your password

[Forgot Your Password?](#)

This is an automated address that is not monitored for replies. In order to contact the sender, you must open the above link first.

 Message Details:

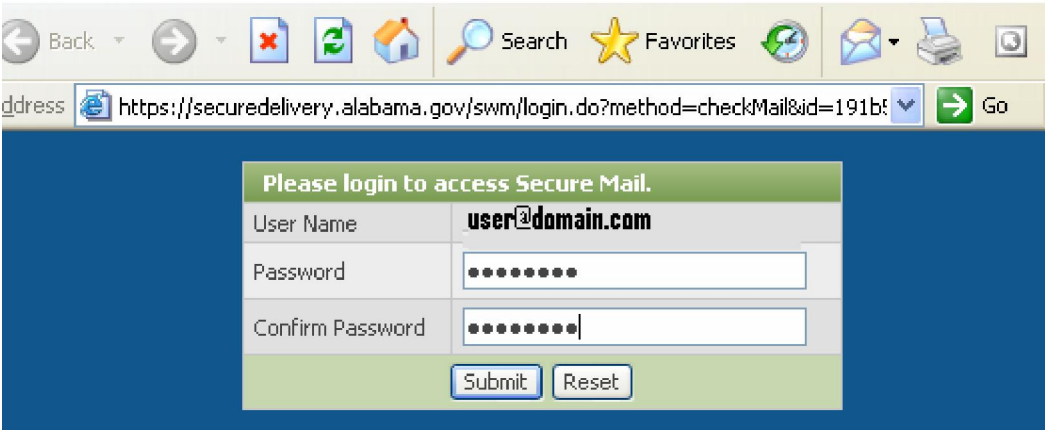
From:

To:

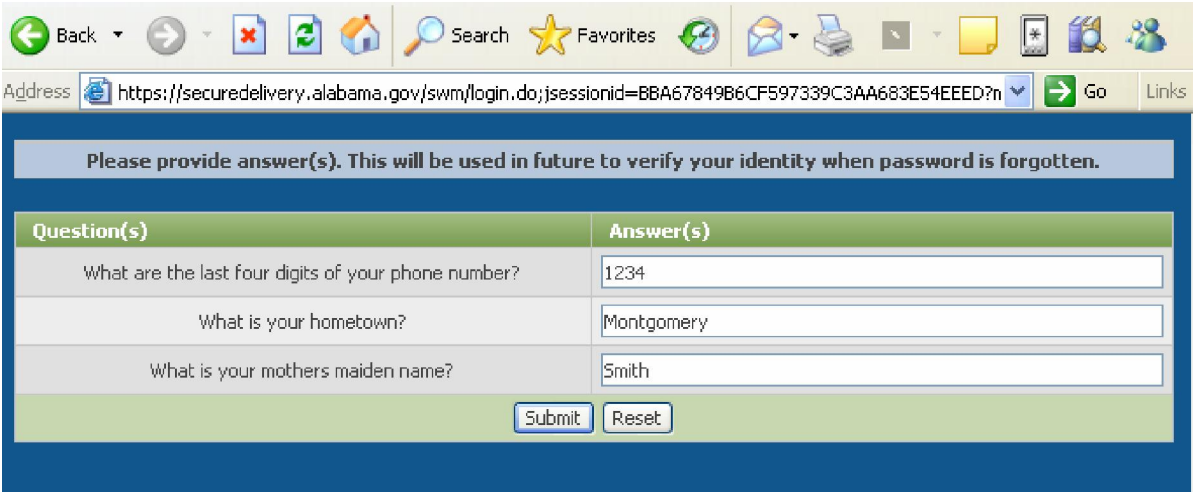
Subject: [encrypt] SSN included

For support, please email help_desk@isd.alabama.gov or call (334)242-2222.

This form will contain relevant information to help the recipient recognize the sender.



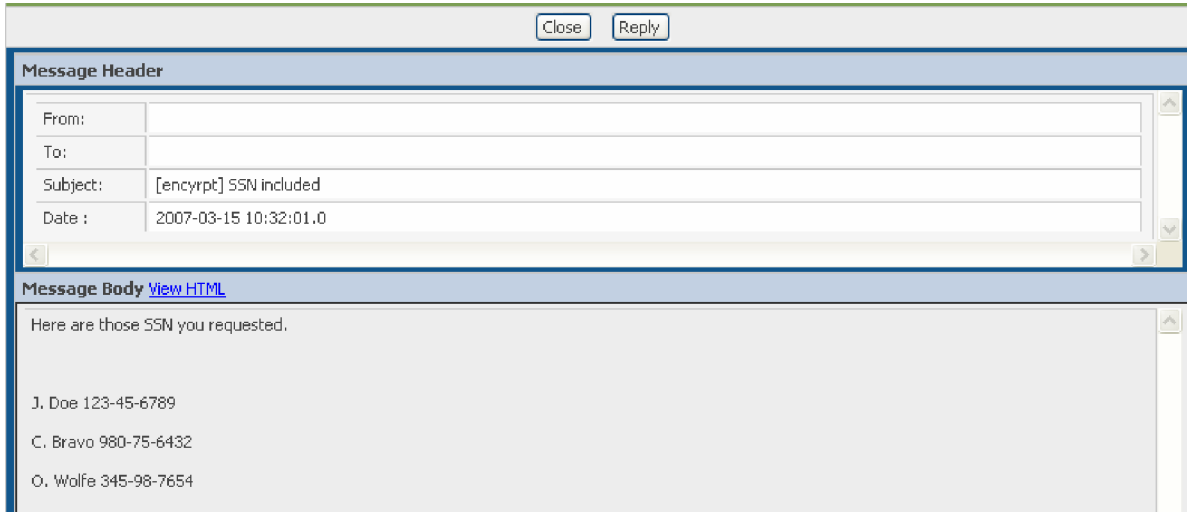
The first time a recipient accesses SWD, they will need to create a password...



Question(s)	Answer(s)
What are the last four digits of your phone number?	1234
What is your hometown?	Montgomery
What is your mothers maiden name?	Smith

and they will need to provide challenge responses in case they forget their password.

Once they have entered the appropriate credentials, the recipient can view the message you sent. Replies can also be sent back securely to the original sender. Any reply sent through SWD is limited to a maximum size of 10MB.



The screenshot shows an email client interface. At the top, there are 'Close' and 'Reply' buttons. Below them is a 'Message Header' section with fields for 'From:', 'To:', 'Subject:', and 'Date:'. The 'Subject' field contains '[encrypt] SSN included' and the 'Date' field contains '2007-03-15 10:32:01.0'. Below the header is a 'Message Body' section with a 'View HTML' link. The body text reads: 'Here are those SSN you requested.' followed by a list of names and SSNs: 'J. Doe 123-45-6789', 'C. Bravo 980-75-6432', and 'O. Wolfe 345-98-7654'.

After the recipient is done reading your message, they have the option of deleting it. If they do not delete the message, it will automatically be deleted after two weeks. Any message that has not been read in two weeks will be automatically deleted too.

Please keep in mind that SWD is only a valid option for emails that leave our system through the outbound gateways. If you want to send an encrypted message to another State of Alabama employee, you will first need to exchange public keys with them via a digital signature. The first step in this process is to request a Security Certificate.

ISD provides a Certificate Server free of charge to users on our network. Users not on our network will either need to get a certificate from a different Certificate Authority or use the steps below for externally-requesting a certificate.

How to Request a Certificate (Internal Users)

1. On the client machine, open a web browser and go to <http://acecertroot.al.mail/certsrv/>.
2. When prompted for credentials, enter your email user name and password. **NOTE** You must include the domain in your user name (*Domain\FristName.LastName*).



3. Click Request a Certificate.
4. Click User Certificate.
5. Click Submit. Depending on your Internet Security settings, you may get a notification that a new certificate is being installed. If you see this message, click Yes.
6. Click Install this Certificate. You may get another notification here. Click Yes on it too.

How to Request a Certificate (External Users)

The certificate server is not accessible from outside of our network because of security concerns. In order to obtain a certificate, you will either need to provide your password to an administrator inside the network, or your password will have to be reset by an administrator.

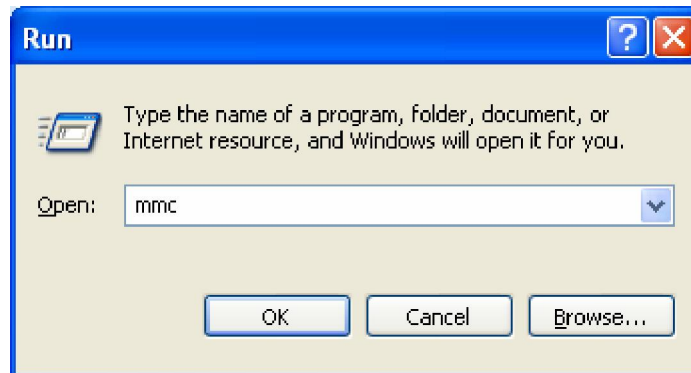
The below steps will need to be completed by the internal administrator.

1. On your machine, open a web browser and go to <http://acecertroot.al.mail/certsrv/>.
2. When prompted for credentials, enter the user name and password for the End User in question. ****NOTE**** You must include the domain in your user name (*Domain\FristName.LastName*).

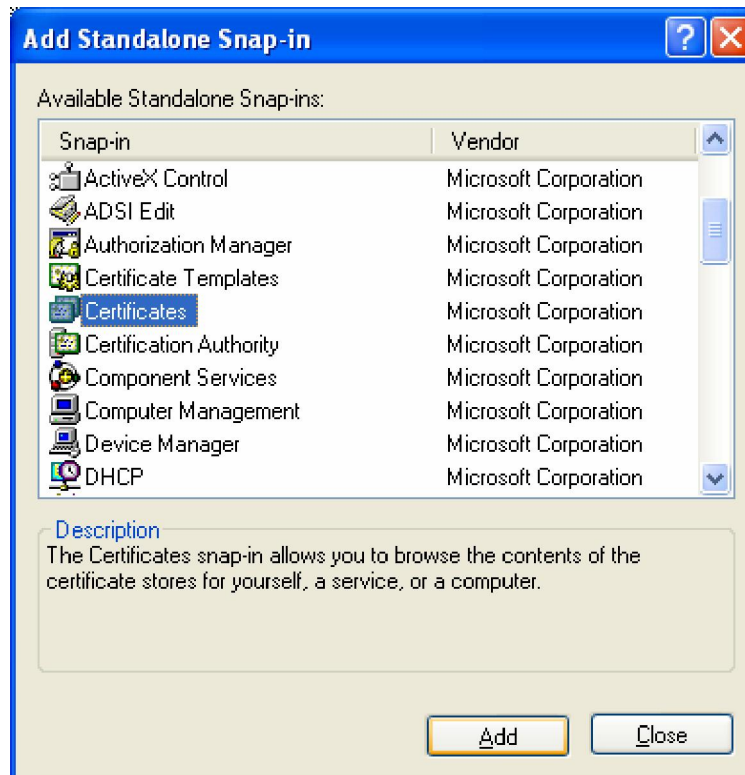


3. Click Request a Certificate.
4. Click User Certificate.
5. Click Submit. Depending on your Internet Security settings, you may get a notification that a new certificate is being installed. If you see this message, click Yes.

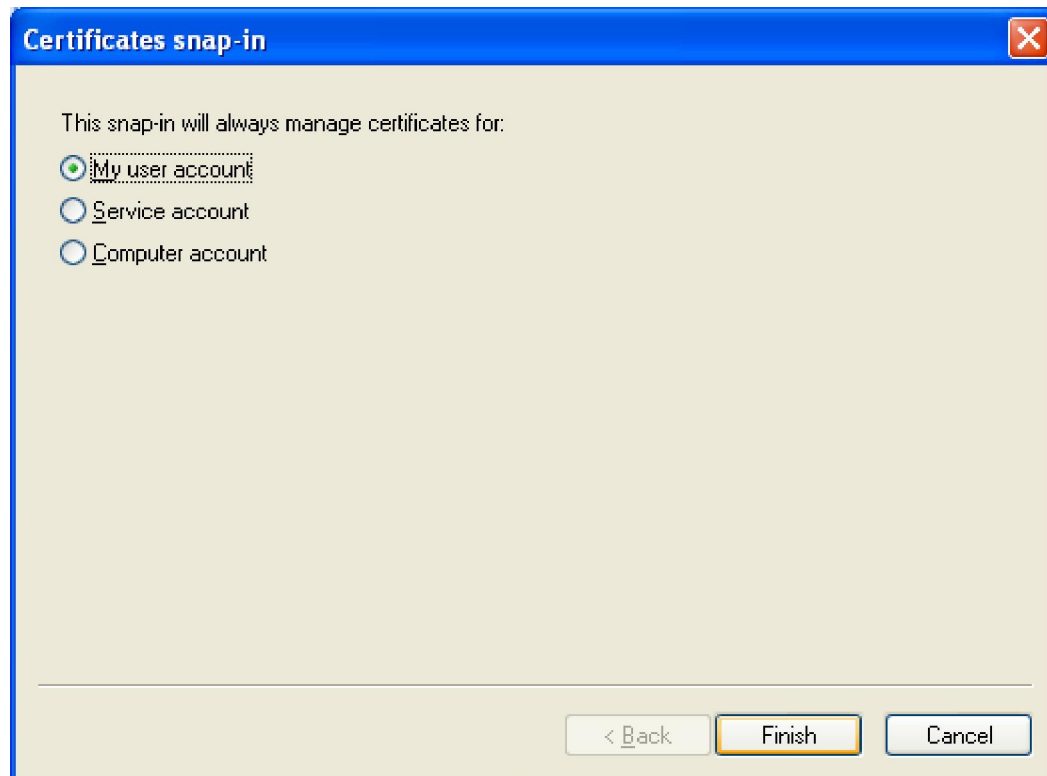
6. Click Install this Certificate. You may get another notification here. Click Yes on it too.
7. On your desktop, click Start > Run and type MMC.



8. In the new console window that opens up, click File > Add/Remove snap-in... Then click the Add button.
9. Highlight Certificates and click Add.



10. Make sure My user account is selected and click Finish. Then click Close. Then click OK.

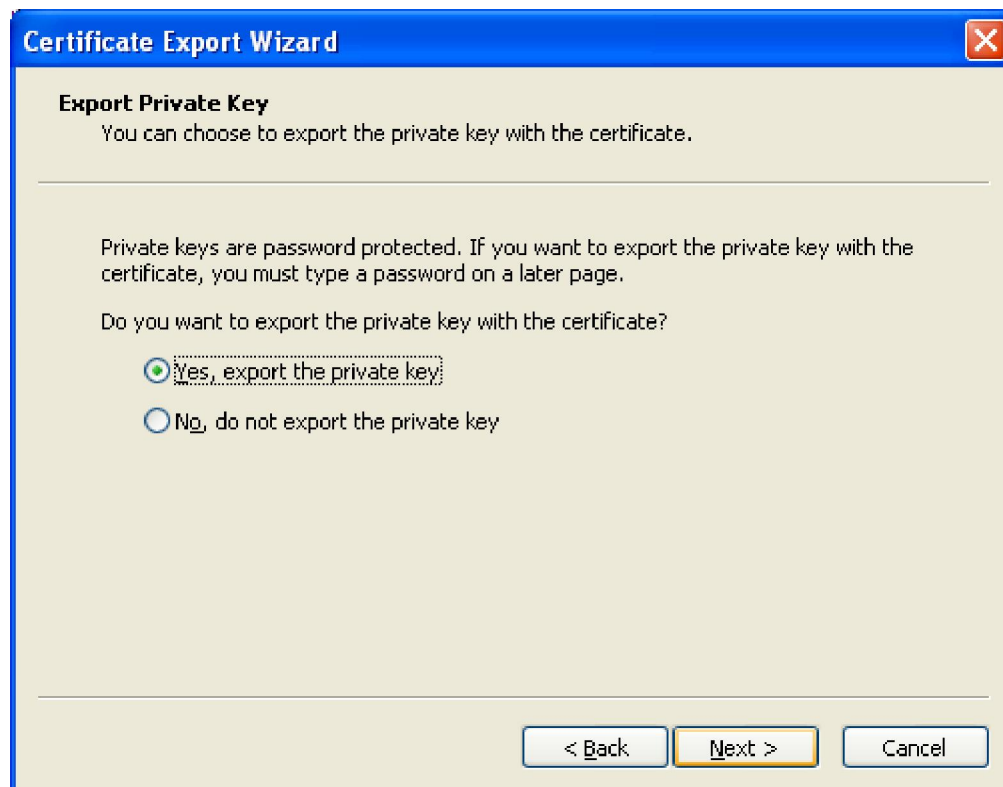


11. You should now be looking at the Certificates Management Console for Current User. Browse down to the Personal folder and double-click Certificates.

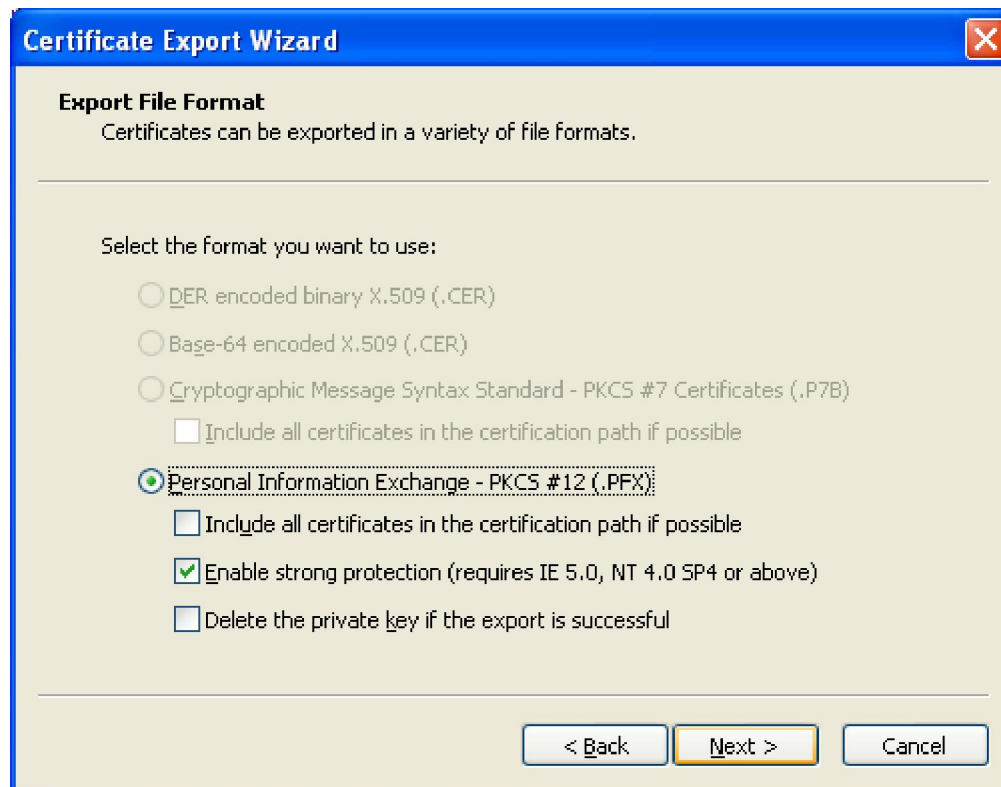


12. Highlight the user in question and then in the Action menu, point to All Tasks and click Export.

13. In the Certificate Export Wizard, click Yes, export the private key. (This option will appear only if the private key is marked as exportable and you have access to the private key.) Then click Next.



14. Under Export File Format, do one or all of the following, and then click Next.
- To include all certificates in the certification path, select the Include all certificates in the certification path if possible check box.
 - To enable strong protection, select the Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above) check box.
 - To delete the private key if the export is successful, select the Delete the private key if the export is successful check box.

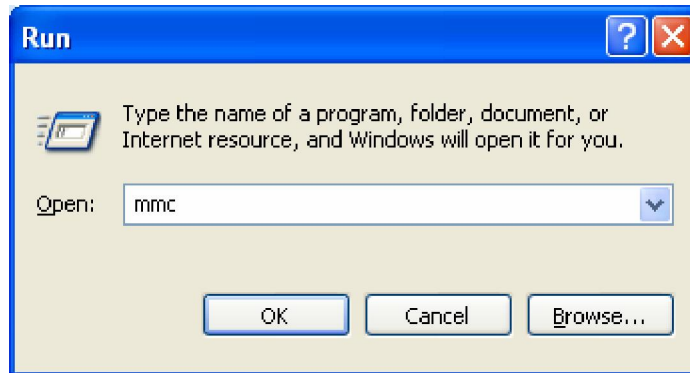


ISD recommends you only check "Enable strong protection"

15. In Password, type a password to encrypt the private key you are exporting. In Confirm password, type the same password again, and then click Next.
16. In File name, type a file name and path for the PKCS #12 file that will store the exported certificate and private key, click Next, and then click Finish.
17. Email the *.pfx file and the password you used for it to the External User.

The below steps will need to be completed by the external user.

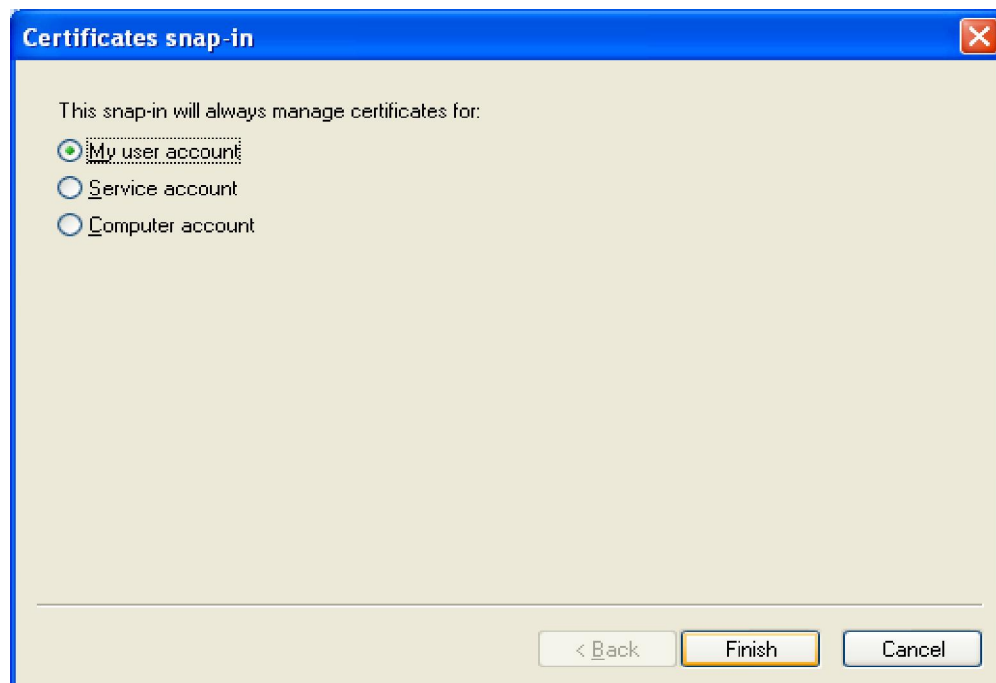
1. Open up the email from your administrator that contains the new certificate and save the file to your C:\.
2. On your desktop, click Start > Run and type MMC.



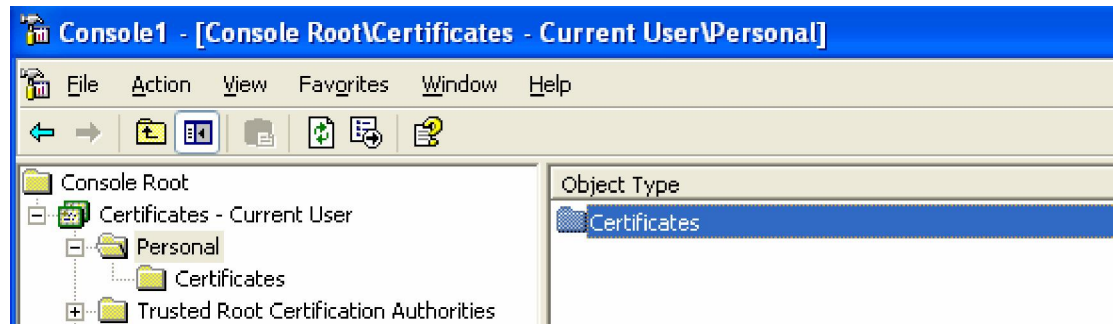
3. In the new console window that opens up, click File > Add/Remove snap-in... Then click the Add button.
4. Highlight Certificates and click Add.



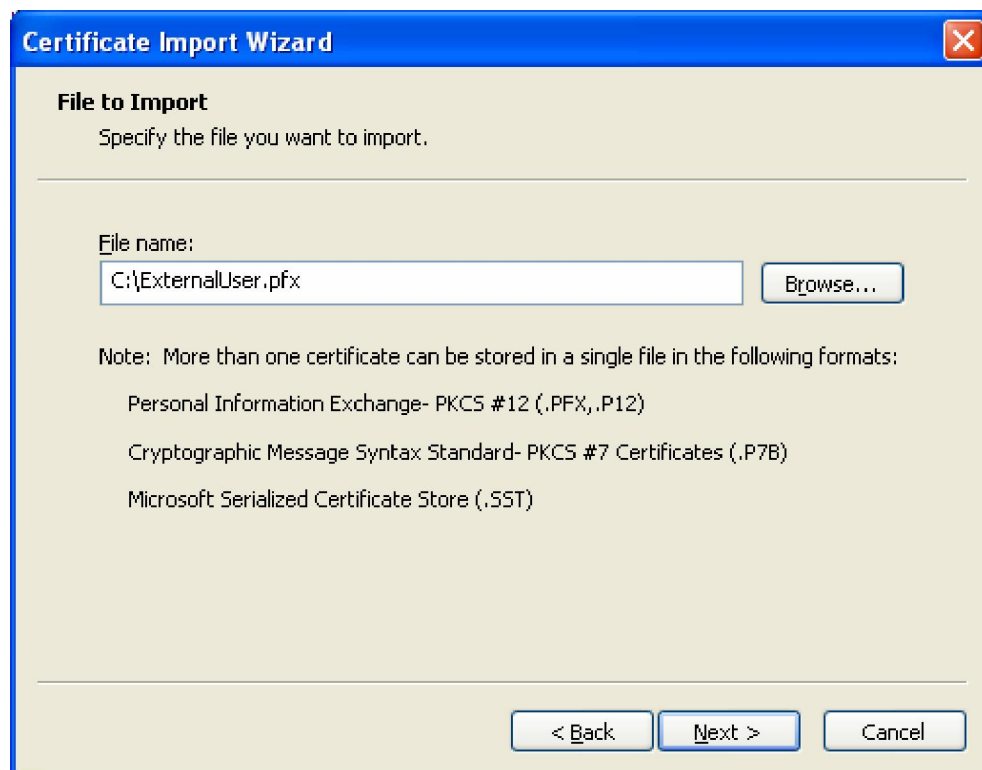
5. Make sure My user account is selected and click Finish. Then click Close. Then click OK.



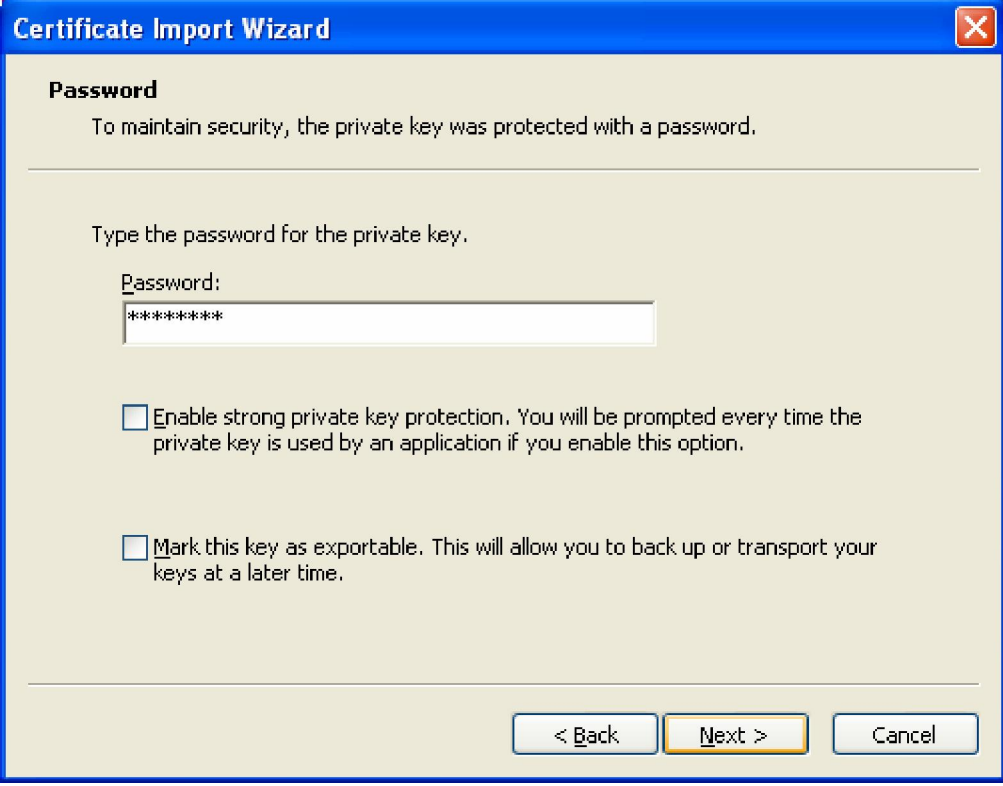
6. You should now be looking at the Certificates Management Console for Current User. Browse down to the Personal folder and double-click Certificates.



7. On the Action menu, point to All Tasks and then click Import to start the Certificate Import Wizard.
8. Click Browse... to navigate to your C:\ and select the file you saved in step 1. **NOTE** You will need to change the Files of Type drop down box to All Files (*.*) .

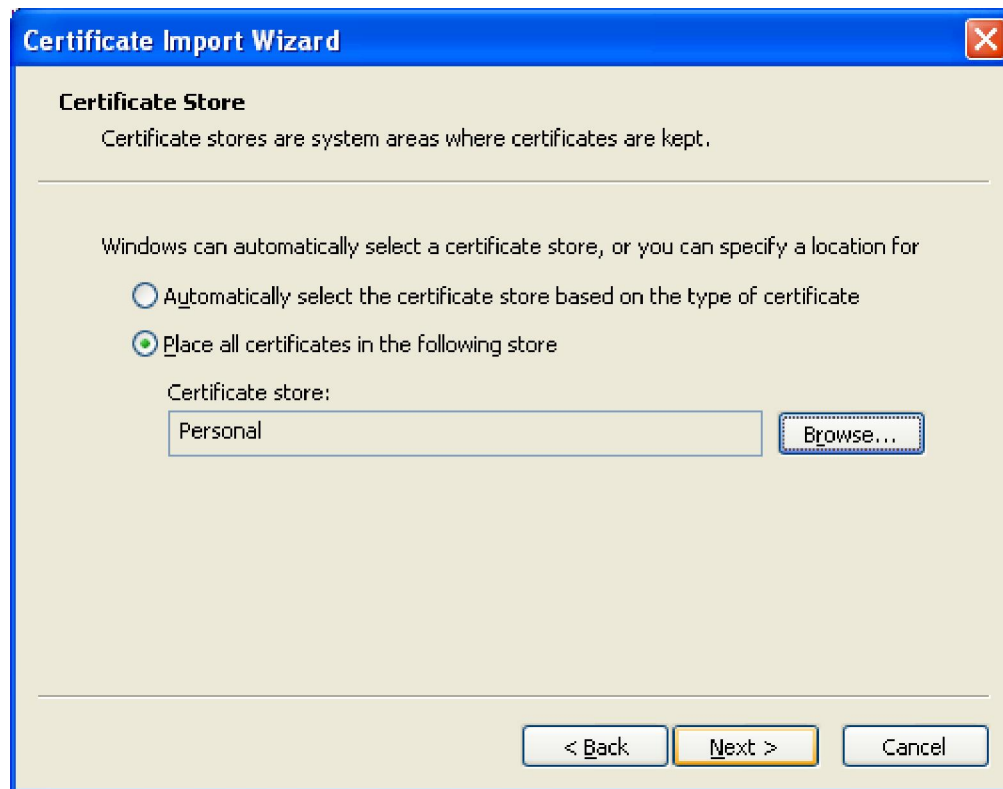


9. Enter the encryption password assigned by your administrator and click Next.



The image shows a Windows-style dialog box titled "Certificate Import Wizard". The window has a blue title bar with a close button (X) in the top right corner. The main area has a light beige background. At the top, the word "Password" is in bold. Below it, a message states: "To maintain security, the private key was protected with a password." A horizontal line separates this from the next section. The text "Type the password for the private key." is followed by a label "Password:" and a text input field containing seven asterisks "*****". Below the input field are two unchecked checkboxes. The first checkbox is labeled "Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option." The second checkbox is labeled "Mark this key as exportable. This will allow you to back up or transport your keys at a later time." At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a yellow border), and "Cancel".

10. Select Place all certificates in the following store, click Browse, and choose Personal. Then click Next.



11. At the Completing the Certificate Import Wizard page, click Finish.

Now that you have a Security Certificate, you can add a Digital Signature to your emails, or publish it to the Global Address List (GAL). Once you have exchanged digital signatures with another user, (either internal or external) you can send encrypted messages back and forth.

To Publish your Digital Signature to the GAL

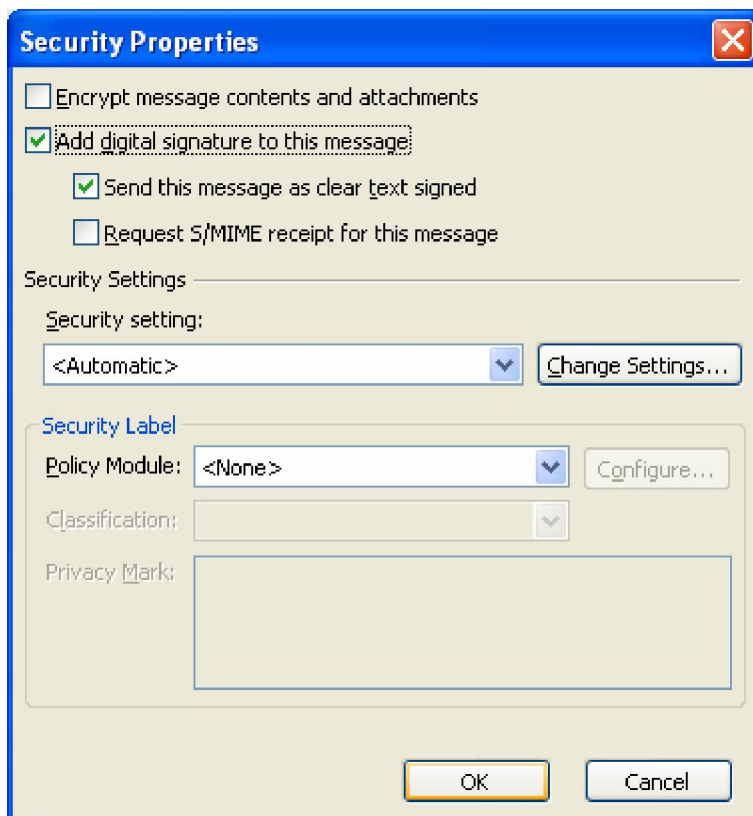
In Outlook, go to Tools > Options and click on the Security tab. Click on the Publish to GAL button. When you see the Microsoft Office Outlook pop-up appear, click OK.



To Attach your Digital Signature to an Email

In the message, click the Options menu. Then click Security Settings. Place a check mark in the Add digital signature to this message checkbox. If you want recipients who do not have S/MIME security to be able to read the message, select the Send this message as clear text signed check box. By default, the check box is selected.

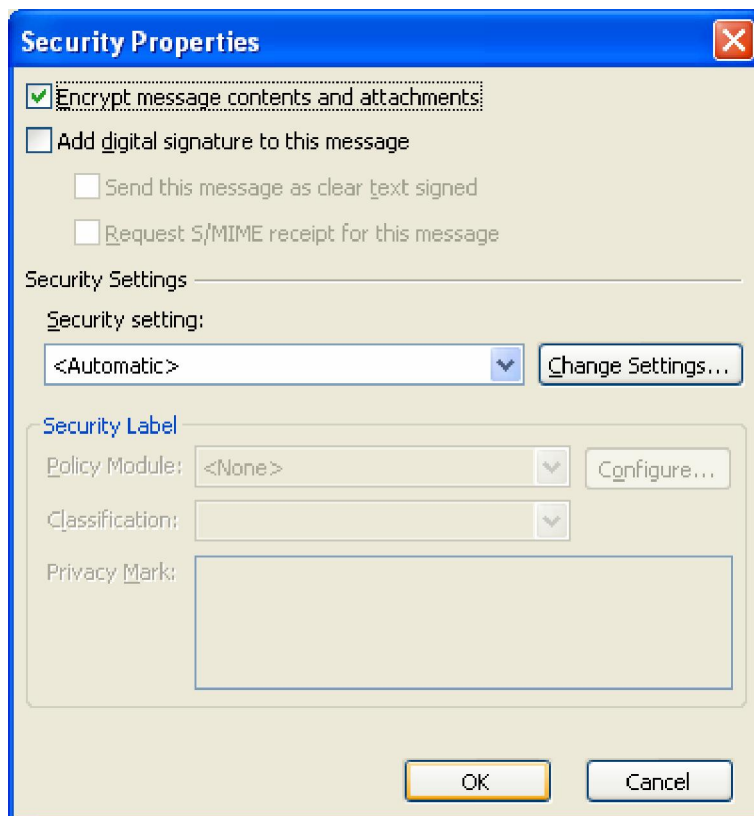
To verify that your digital signature is being validated by recipients and to request confirmation that the message was received unaltered, as well as notification telling you who opened the message and when it was opened, select the Request S/MIME receipt for all S/MIME signed messages check box. When you send a message with an S/MIME return receipt request, this verification information is returned as a message sent to your Inbox.



Sending an Encrypted Message through Outlook

In order to use the Encrypt Message feature in Outlook, you must first exchange digital signatures with the intended recipient so you both have each other's public key. Add the intended recipient into your contacts, either from the GAL or the message they sent you with their digital signature. They will need to do the same. You can verify you have a certificate for one of your contacts by opening up the contact and clicking on the Certificates tab.

Once this is completed, you can now use Outlook's Encrypt Message feature by clicking on the Options menu in any message. Then click the Security Settings button. Place a checkmark in the Encrypt message contents and attachments checkbox.



Using S/MIME Controls in Outlook Web Access (OWA)

The Encrypt Message and Digitally Sign features work slightly different in OWA than Outlook. Before you are able to use these features, you must install the OWA S/MIME controls. To do so:

1. On the client computer, open a web browser and go to www.webmail.alabama.gov, and logon to Webmail normally.
2. In the OWA Navigation pane, click Options.
3. Under Email Security, click Download. If you receive a Security Warning dialog box, click Yes.

Just as with Outlook, before you can send an encrypted message to a recipient, you must exchange public keys. This is still done with Digital Signatures. Begin by creating a new message to the desired recipient. Click the Add a digital signature to this message button along the top and send the message. The recipient will need to reply to this message with their own digital signature. Add this user into your contacts.

Now compose a new email to the recipient. Click the Encrypt message contents and attachments button along the top. Send the message as normal.